Place for Hope Employee Privacy Notice
updated version 3; approved December 2021

Place for Hope (Charity Number: SC045224) ("Employer" "our" or "we") act as a data controller in respect of your personal information and this means that we are responsible for deciding how we hold and use personal information about you. We collect and process personal data relating to our employees to manage the employment relationship. We are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

This Privacy Notice applies to current and former employees (also referred to as "you" or "your"). Please note that this Privacy Notice does not form part of any contract of employment, or other contract to provide services.

The person with responsibility for data protection compliance is Helen Boothroyd: helen.boothroyd@placeforhope.org.uk. For any data breaches involving staff or complaints about how your personal data has been handled, please contact the Director Carolyn Merry: carolyn.merry@placeforhope.org.uk; 07810 208 894.

What is 'personal information'?
Your 'personal information' means any information about you from which you can be identified - either by reference to an identifier (for example your name, location data or online identifier (e.g. IP address) or from factors specific to your physical, cultural or social identity (e.g. your social background, outside interests etc).

It does not include information where the identity has been removed (such as anonymous information).

What personal information do we collect and process?
We collect and process a range of information about you. This may include (but is not limited to):

- your name, address and contact details (work and personal), including email address and telephone number, date of birth and gender, marital status, dependents, next of kin and emergency contact information;
- the terms and conditions of your employment, including your job title and workplace;
- photographs / film footage;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with us, and any other information included in an application form or covering letter as part of the application process;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account, payroll records, tax status information and national insurance number;
- information about your entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;

- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details about maternity, paternity, parental and adoption leave and necessary relevant information to manage your leave;
- voicemails, e-mails, correspondence, documents, and other work product and communications created, stored or transmitted using our networks, applications, devices, computers or communications equipment;
- information about your use of our information and communications systems, including monitoring thereof;
- health and safety information (this can form photographs, videos, investigation notes, health reports, witness statements);
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence; and
- assessments of your performance, training records, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence.

'Special Category' Information
We will also collect and process 'special category' information about you, which is information that is more sensitive (such as information about racial/ ethnic origin, sexual orientation, political opinions, religious/ philosophical beliefs, trade union membership, biometric or genetic data and health data) and given a higher level of data protection laws. This may include (but is not limited to):

- information about medical or health conditions, including whether or not you have a disability for which we need to make reasonable adjustments;
- information about your religion, either provided voluntarily as part of an application or because required in accordance with the Equality Act 2010 Sch. 9, Para 3;
- information about your nationality; and
- criminal convictions information.

How do we collect your personal information?
We collect this information in a variety of ways. For example, data is collected through application forms; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments.

In some cases, we may collect personal data about you from third parties, such as references supplied by former employers, medical officers, information from criminal records checks permitted by law, credit reference agencies or other background check agencies. The categories of personal information we may collect, store and use from third parties include (but are not limited to) the following categories of information:

- References
- Occupational health reports
- Criminal record check results

Throughout the period you are working for us, we may collect additional personal information about you, including from your line manager, other managers and colleagues (e.g. feedback on your performance as part of the annual appraisal process).

What is the legal basis?
In most cases, we will process your personal information where it is necessary:

- to perform the contract we have entered into with you for the purposes of employment (for example, we need to process your personal information to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit and pension entitlements) – **Basis 1**
- to ensure that we are complying with our legal obligations (for example, we are required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled). For certain positions, we may be required to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question – **Basis 2**
- for our legitimate interests in processing personal information before, during and after the end of the employment relationship – **Basis 3;**
- when we have obtained your consent (for example, if we are making travel arrangements on your behalf we will pass this information to the travel providers) – **Basis 4**.

Where we rely on legitimate interests as a reason for processing personal information, we have considered whether or not those interests are overridden by the rights and freedoms of employees or workers and we have concluded that they are not. Our legitimate interest is the purpose for which we process the data (e.g. for data we process during the recruitment process, the legitimate reason for processing that data is recruitment).

We may also process your personal information in the following circumstances, but this is likely to be rare:

- with your specific consent;
- where we need to protect your interests (or someone else's interests);
- where it is needed in the public interest.

If we are processing special category data or criminal convictions data we may also rely on the following conditions in addition to the legal bases above:

- where you have given your consent to the use of your data;
- where we are required to process your data in the public interest for the purposes of safeguarding children and individuals at risk or regulatory requirements relating to unlawful acts and dishonesty;
- where we are required to process your data in the public interest for the purposes of equal opportunities or treatment.

What is the purpose for processing your personal information?
Processing your personal information allows us to do a number of different purposes, including, but not limited to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the we comply with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- comply with our legal obligations, such as health and safety laws;
- respond to and defend against legal claims; and
- maintain and promote equality and diversity in the workplace.

We will only use your personal information for the purposes for which we collected it - unless we reasonably consider that we need to use it for another purpose that is compatible with the original purpose.

If we need to use your personal information for an unrelated purpose, we will notify you and explain the basis upon which that is necessary.

What is the purpose for processing 'special category' personal information?
Some special categories of personal data, such as information about health or medical conditions/diagnoses, is processed to carry out employment law obligations, such as those in relation to employees with disabilities and for health and safety purposes. Processing may also be necessary for the purposes of preventive or occupational medicine or for the assessment of the working capacity of the employee. This will be the case when managing ill health or carrying out occupational health assessments.

We may need to process information about religion, which is a special category of data, for jobs which require the post holder to be a member of a faith community in accordance with

the Equality Act 2010 Sch. 9, Para 3 and to ensure meaningful equal opportunity monitoring and reporting. In other instances, employees are entirely free to decide whether to provide such data, on application forms or subsequently, and there are no consequences of failing to do so.

Consent

We will only seek and rely on your consent where you are fully informed and your consent can be freely given.

There may be limited circumstances where we will approach you to obtain your explicit consent to allow us to process certain particularly sensitive data, or other personal information.

If so, we will provide you with full details of the information that we require and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that you do not have to provide your consent and it will not impact on your contract with us if you do not consent.

You have the right to withdraw your consent for that specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for that purpose.

If you wish to withdraw your consent, please contact Carolyn Merry: carolyn.merry@placeforhope.org.uk.

Who do we share your personal information with?
Your personal information will be shared internally, including with your line manager and with other staff if access to the data is necessary for performance of their roles. We may also need to share your personal information with volunteers, including Practitioners, trustees and volunteers assisting with financial systems, if access to the data is necessary for performance of their roles..

Third Parties
We contract with third party service providers and suppliers to deliver certain services. Our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We are also legally required to transfer certain data to governmental and regulatory bodies.

We may share your personal information with third parties in order to get pre-employment references. We may also obtain necessary criminal records checks from the Disclosure and Barring Service or Disclosure Scotland.

We may also share your personal information with third parties that process data on our behalf, predominantly in connection with payroll, pensions and the provision of benefits.

The following third parties may have access to your personal information for the purposes noted below:

- Microsoft hosts our emails on Outlook in Office 365 and any documents stored to Office 365 applications, processing personal data in the UK;
- Dropbox hosts our file storage, processing personal data in the US;
- Mailchimp, which we use for e-newsletters, processing personal data in the US;
- Salesforce hosts our cloud-based database, processing personal data in the UK and US;
- Hootsuite manages our social media interactions, processing personal data in the UK and Canada;
- third-party providers to manage payments, bookings or registrations, e.g. Stripe, Eventbrite, and Google suite, processing personal data in the UK, EU, and US;
- third-party providers to manage our website functions, e.g. Expression Engine and Google Analytics processing personal data in the UK, EU, and US;
- Intego, which is our anti-virus provider, processing personal data in the UK and US;
- Vodafone which is our mobile telephone provider;
- Easybooks accounting system, processing personal data in the UK and US;
- our independent examiner and accountant who is currently Paul Clelland Accountancy, processing personal data in the UK;
- our insurance providers who are currently Keegan and Pennykid, processing personal data in the UK;
- our current account banking providers who are currently CAF Bank, processing personal data in the UK;
- our funders or other grant providers where required e.g. personal information for funding applications or required for reporting on outcomes and outputs;
- any other person who is authorised to act on your behalf (for example, the NHS and/or family members);
- any relevant dispute resolution body or the courts;
- persons or organisations in connection with any merger, disposal, reorganisation, or similar change in our charity;
- HMRC; HSE; regulators, government departments, law enforcement authorities, tax authorities, professional advisers, financial institutions, and insurance companies;
- third parties providing a reference about you, where you have agreed that we can request this or have asked us to request it;
- the Disclosure and Barring Service and Disclosure Scotland in respect of criminal convictions data, processing personal data in the UK;
- the trustees of the pension scheme to which you are a member;
- Nest Corporation who are your pension providers, processing personal data in the UK and EU;
- our payroll providers who are currently QTAC, processing personal data in the UK;
- our HR consultant who is currently Caroline Rochford Consulting, processing personal data in the UK;

- if you move on and require a reference, we will provide your information to your new employer or other body to whom you have asked us to supply it.

Our service providers change from time to time and we will inform you if this is the case. We will not sell, trade or lease your personal information to others.

Legal Basis
In most cases, we will share your personal information with third parties where:

- required by law
- it is necessary to administer the working relationship with you, or
- we have another legitimate interest in doing so, as a business and as your employer

In these circumstances, we require third parties to ensure the security of your personal information and to treat it in accordance with the law.

How do we keep your personal information secure?
Data is stored in a range of different IT systems (including the organisation's email). We use encrypted systems for online processing and storage and anti-virus protection on all staff laptops. All laptops and mobile phones used by our staff are password protected with auto-lock facilities enabled. Email security is a priority, and staff and practitioners are asked to avoid sharing personal information by email.

Our password policy requires:

- The use of complex passwords which would be hard to guess;
- Secure password storage;
- Password sharing between staff as an exception, only where operationally necessary and never regarding the storage of financial or other sensitive information;
- Additional security for financial and other sensitive information, including only password hints being held in secure storage and multi-factor authentication.

Personal information is only accessible to staff members who require it to perform their role. Personal information is only shared with volunteers, e.g. Practitioners, trustees or volunteers assisting with financial systems, only where a specific piece of information is required for the task they are being asked to perform. Volunteers do not have access to our database.

Personal information is not generally held in hard copy. Any hard copy personal information that is required to be held is:

- stored by only one person if possible;
- stored in a locked container;
- shredded at the end of the retention period.

For how long do we keep your personal information?
The following timescale outlines the retention and disposal of all employees and workers records:

a Recruitment Records – held for full duration of employment of the staff member [and for a period of 7 years after the staff member has left employment];
b Payroll, salary, benefit data – 7 years;
c Maternity, paternity, shared parental leave pay records – 7 years;
d Criminal record checks – deleted promptly after the information has been verified;
e Personal files – retained 7 years after the staff member has left employment;
f Finance Records – retained 7 years;
g Certain records held for a number of years after the staff member has left employment. For example:
- Health and safety records – up to 10 years or more depending on the type of record;
- Any records which may be required to prepare for, or defend, a legal claim.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Monitoring
The work output of our employees, whether in paper record, computer files, or in any other storage format belongs to us, and that work output, and the tools used to generate that work output, are always subject to review and monitoring by us, pursuant to our 'use of email, internet and telephones policy' contained in our Employee Handbook.

This section is not meant to suggest that all employees will in fact be monitored or their actions subject to constant surveillance. We have no duty to so monitor. It is meant to bring to your attention the fact that such monitoring may occur and may result in the collection of personal information from employees (e.g. through their use of our resources). When using our equipment or resources employees should not have any expectation of privacy with respect to their use of such equipment or resources.

What if you do not provide personal data?
You have some obligations under your employment contract to provide us with personal data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide us with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable us to enter a contract of employment with you. If you do not provide other information when requested, for example as part of the staff appraisal process, this may hinder our ability to administer the rights and obligations arising as a result of the employment relationship efficiently. Therefore, if you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our staff).

Your rights in relation to your personal information

You have rights in relation to the personal information that we hold about you, including the right:

- to request access to any personal information we hold about you - or in some cases, to obtain a portable copy of it or to have it transferred to a third party;
- to ask to have inaccurate data amended;
- to erase your personal information, or to restrict or challenge the processing of your personal information in limited circumstances;
- to object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms;
- to request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:
  (a) if you want us to establish the data's accuracy;
  (b) where our use of the data is unlawful but you do not want us to erase it;
  c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
  (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it;
- to withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent;
- to lodge a complaint with the Information Commissioner's Office (the UK supervisory authority for data protection issues).

If you want to make one of these requests, please put your request in writing to Carolyn Merry: Carolyn.merry@placeforhope.org.uk.

Please note, we may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We may not always be able to comply with your request to exercise your rights for specific legal reasons which will be notified to you, if applicable, at the time of your request.

If a data subject access request (DSAR) is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A DSAR is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If we consider this to be the case, we will notify you of this and of whether or not we will respond to the request.

Where do we store your information?

The data that we collect from you will usually be stored inside the UK or the European Economic Area (EEA).

However, if you live or work outside of the UK or the EEA, we may need to transfer your personal data outside of the UK or the EEA to correspond with you. If we organise international travel on your behalf we may be required to provide information to providers and government bodies based outwith the EEA.

We also may transfer data outside the UK or the EEA where our service providers host, process, or store data outside the UK or the EEA. Where we do this, we will ensure that the transfer is to a country covered by a decision of the UK and/or European Commission or is otherwise made in circumstances where appropriate safeguards are in place to protect your data in accordance with the UK data protection legislation (e.g. standard contractual clauses, EU-US Privacy Shield compliant, etc.).

Review

This privacy notice will be reviewed annually, but we may update, or otherwise amend, this Privacy Notice at any time.

This document was last updated on 10 November 2021. It was considered and recommended for approval by the Policy and Practice Forum on 15 November 2021 and approved by the Board of Trustees on 7 December 2021.

Contact

If you have any questions regarding this Privacy Notice, how we handle your personal information or you would like to update the information we hold about you, please contact Helen Boothroyd: helen.boothroyd@placeforhope.org.uk.

If you are unhappy about how we process your personal data, you can:

- submit a complaint to Carolyn Merry: Carolyn.merry@placeforhope.org.uk.; or
- notify the Information Commissioner's Office (ICO) by calling their helpline on: 0303 123 1113.